Security Futures

Paul Falde, Cray Research, Inc., Eagan, Minnesota

ABSTRACT: *At the Tours CUG, Cray Research, Inc. presented some potential direction changes with respect to UNICOS Multilevel Security (MLS) systems. Plans have now solidified, and this paper is an update on Cray's future strategies for UNICOS MLS systems.*

Introduction

As presented at the Tours France CUG, Cray Research, Inc. was in the midst of evaluating the future direction of the UNICOS MLS system. At that time, a number of alternatives were presented.[1] During that CUG, and since then, Cray has received a lot of feedback about those alternatives.

After careful consideration of customer input and Cray's limited resources, priorities were determined and plans were established. This paper discusses the plans, which reflect Cray's ongoing commitment to enhanced UNICOS security features.

Trusted UNICOS Support for CRAY T3D Systems

Full Trusted UNICOS functionality will be implemented for CRAY T3D systems in the UNICOS MLS 8.0.4 and the UNICOS MAX 1.2 releases. This will allow customers to integrate the CRAY T3D system into a trusted environment and have the benefit of the B1 networked-security functionality. However, there will be no formal evaluation of this configuration.

CIPSO Performance

At the Tours CUG, concern was expressed about poor performance with the Common Internet Protocol Security Option (CIPSO). CIPSO performance in UNICOS MLS 8.0 systems was found to be approximately 10% of the performance of the non-CIPSO IP (Internet Protocol). Cray has investigated this problem, and it is fixed for UNICOS 9.0 systems. CIPSO performance is now about 95% of non-CIPSO IP.

Merging UNICOS non-MLS and MLS Systems

The UNICOS MLS configuration is currently optional, and it is selected during system installation. Plans for the UNICOS 10.0 system include folding the MLS functionality into the UNICOS base system, thereby eliminating the need for this configuration option. Combining these two UNICOS configurations makes more security features available to all customers (security auditing, access control lists (ACLs), etc.), but use of the features is still optional (albeit, the use of ACLs is left to the discretion of each user). The merging of these configurations also frees up resources to allow deeper testing of the base UNICOS configuration.

Trusted Facility Management (TFMgmt)

The UNICOS 7.0 MLS TFMgmt style of security policy (PRIV_TFM) was preserved in UNICOS 8.0 and will be in UNICOS 9.0, but it will be eliminated beginning with the UNICOS 10.0 release. Customers who are using a PRIV_TFM system will need to migrate to either a combination of superuser/separate administrative role, or a separate administrative role (Privilege Assignment List (PAL)-only configuration) policy during UNICOS 9.0.

In a PRIV_TFM configuration, the administrative roles of operator, system administrator, and security administrator were separated, but two fundamental design problems exist with this implementation. PRIV_TFM does not support a true separation of administrative roles, and when used in a multilevel security environment (non-zero security labels are in use), many system utilities function incorrectly. The UNICOS software supported by PALs resolves these issues.

The UNICOS 10.0 system will support both an all-powerful superuser role as well as distinct operator and administrator roles. The administrator-role policy will be supported via PALs. Regardless of the security policy in use, PALs will be in the system. On systems using only a superuser policy, PALs should be transparent, but administrators will need to be aware of their existence.

There is an issue that must be considered when customers are making a decision on which TFMgmt policy to migrate. Only a subset of UNICOS software is supported by PALs. This is basically the set described by Trusted UNICOS 8.0 and Trusted UNICOS 9.0 configurations.

[1] Refer to "Security and Microkernel Technology" written by Paul Falde in the 1994 Fall CUG Proceedings for additional information.

Trusted UNICOS

The Trusted UNICOS product was initially introduced with UNICOS 8.0. It supported the U.S. Department of Defense (DoD) B1 criteria for Trusted Systems, and was successfully evaluated and rated by the National Security Agency (NSA) as a network operating system. Although support for the Trusted UNICOS configuration continues, only the very first version of the 8.0 release is formally considered to be an evaluated product, and Cray has no plans for a future re-evaluation. Cray plans to continue support in UNICOS 10.0 for the functionality provided by Trusted UNICOS systems, but the Trusted UNICOS configuration option will be removed at that time. All references to Trusted UNICOS as a configuration will be dropped from UNICOS 10.0 documentation.

Security Configuration Options Reduced

To reduce development and testing costs, the number of configuration options related to security will be reduced in UNICOS 10.0. (Note: full support for all the auditing configuration options will continue.)

The configuration options that might be deleted are:

FSETID_RESTRICT
MAC_COMMAND
MLS_INTEGRITY
PRIV_TFM
SECURE_MLSDIR
SECURE_MOUNT
SECURE_REMOTE
STAT_RESTRICT

Removal of these configuration options could potentially cause migration issues for sites upgrading from UNICOS MLS 9.0 to UNICOS 10.0. Cray is currently accepting feedback on the above configuration options. Firm decisions on these options will be made the week following the Denver CUG and will be documented in the *UNICOS 9.0 Release Preview* so customers can prepare appropriately.

More detail for each of these options follows[2]:

FSETID_RESTRICT - when this option is removed, all users will be permitted to manage their own setuid/setgid files, which is equivalent to the current non-MLS UNICOS functionality.

MAC_COMMAND - when this option is removed, subjects will be permitted to view information for an object only when the subject dominates the object, which is consistent with the current MLS MAC policy.

MLS_INTEGRITY - this UNICOS MLS option is not currently used.

PRIV_TFM - (described in the previous section on "Trusted Facility Management (TFMgmt)".)

SECURE_MLSDIR - when this option is removed, a directory's security label can be upgraded only if that directory is empty (assuming the user has appropriate access permissions), which is consistent with the current MLS MAC policy.

SECURE_MOUNT - this option becomes obsolete in UNICOS 10.0 (refer to the previous section on "Merging UNICOS non-MLS and MLS Systems"). That is, all file systems will be labeled. Non-MLS file systems can be mounted on a UNICOS 10.0 system.

SECURE_REMOTE - this UNICOS MLS option is not currently used.

STAT_RESTRICT - when this option is removed, a subject can perform a stat operation only for an object that the subject dominates, which is consistent with the current MLS MAC policy.

MAC will be a Separately Priced Product

Cray is currently developing a plan to begin charging for Mandatory Access Control (MAC) to help cover ongoing development and support costs for this functionality.

Security Policies and Assurance

Cray has a continuing commitment to support consistent security policies and provide a practical level of security assurance. The knowledge base within the Software Division for security practices, policies, and techniques will be increased through an education program for developers, testers, and writers. Security issues require attention in the earliest design stages and throughout a product's life-cycle.

UNICOS/mk Support

The UNICOS/mk operating system is targeted to support future MPP and Scalable Node architectures. Cray plans to port the security functionality of the UNICOS 10.0 release to one of the early releases of the UNICOS/mk system. This project will provide a migration path for those customers who purchase new-technology Cray hardware and need enhanced UNICOS/mk security.

Summary

Cray Research continues to support enhanced security and MLS technologies deemed important by customers for the UNICOS operating system. This support extends from today's software and hardware products to those far into the future.

[2] Where appropriate, restrictions can be bypassed by an authorized administrator.